AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings of claims in the Application.

1. (Currently Amended): A method for utilizing a public wireless local area network (WPAN) for a client with a smart card, comprising:

creating a one-time entropy generated password for a client including:

calculating a hash value based on an identification information of the client, an encryption key provided by the WPAN, and a predetermined text character string, ~~wherein creating comprises calculating a hash value comprising~~, wherein the calculated hash value includes a plurality of octet values; and

subsequently converting any non-alphanumeric octet values of the plurality of octet values of the calculated hash value into an alphanumeric octet value;

storing the one-time entropy generated password and identification information of the client on a public wireless local area network; and

utilizing the one-time entropy generated password and identity information of the client to authenticate the client in the public wireless local area network.

2. (Original): The method of claim 1 wherein the authentication is provided by a Remote Authentication Dial-In User Service (RADIUS) server.

3. (Previously Presented): The method of claim 1 further comprising authenticating the client by a server associated with said WPAN based on a smart card.

4. (Previously Presented): The method of claim 1 further comprising authenticating the client by a server associated with said WPAN based on a universal subscriber identity module card.

5. (Previously Presented): The method of claim 1 further comprising authenticating the client by a server associated with said WPAN based on a subscriber identity module card.

6. (Original): The method of claim 1 further comprising modifying accounting data from the public wireless local area network to include charging data record fields for the client.

7. (Original): The method of claim 1 wherein the creating is independently performed by each of two entities.

8. (Original) The method of claim 1 wherein the creating comprises utilizing international mobile subscriber identity (IMSI) of the client.

9. (Original): The method of claim 1 wherein the creating comprises utilizing a pseudonym of the client.

10. (Previously Presented): The method of claim 1 wherein the creating comprises utilizing Point-to-Point Encryption Send-Key.

11. (Previously Presented): The method of claim 1 wherein the creating comprises utilizing Point-to-Point Encryption Recv-Key.

12. (Canceled).

13. (Previously Presented): The method of claim 1 wherein the creating comprises; calculating a hash value using a SHA-1 hashing process, the hash value comprising a plurality of octet values; and converting any non-alphanumeric octet values of the plurality of octet values into an alphanumeric octet value.

14. (Currently Amended): A system for utilizing a public wireless local area network for a client with a smart card, comprising:

a smart card for a client; and

a first adapter ~~for generating~~ arranged to generate a one-time use password for the client, wherein the one-time use password is generated by generating a hash value based on an identification information of the client, an encryption key provided by the WPAN, and a text character string, wherein the password is used for authenticating the client by a Remote Authentication Dial-In User Service (RADIUS) server, wherein the generated hash value includes a plurality of octet values, and wherein any non-alphanumeric octet values of the plurality of octet values of the generated hash value is converted into an alphanumeric octet value;

~~wherein generating a one-time use password comprises calculating a hash value comprising a plurality of octet values and subsequently converting each of the plurality of octet values of the hash value into an alphanumeric octet value~~.

15. (Original): The system of claim 14 further comprising a second adapter for authenticating the client by a second server based on the smart card.

16. (Previously Presented): The system of claim 15 wherein the first and second adapters reside on separate devices.

17. (Original): The system of claim 15 further comprising a third adapter for modifying RADIUS based accounting data to generate General Packed Radio Server (GPRS) based accounting data.

18. (Previously Presented): The system of claim 17 further comprising a fourth adapter for generating the password for the client.

19. (Currently Amended): A method for adapting a public wireless local area network for a client with a smart card, comprising:

creating a one-time use password for a client including:

calculating a hash value based on information of the client, an encryption key provided by the WPAN, and a text character string ~~identification by calculating a hash value comprising~~, wherein the calculated hash value includes a plurality of octet values; and

subsequently converting any non-alphanumeric octet values of the plurality of octet values of the calculated hash value into an alphanumeric octet value;

~~information of the client, an encryption key provided by the WPAN, and a text character string;~~

storing the password and the identification information on a Remote Authentication Dial-In User Service (RADIUS) server;

utilizing the password and the identification information to authenticate the client on the RADIUS server; and

modifying RADIUS based accounting data to generate General Packed Radio Server (GPRS) based accounting data for the client.

20. (Previously Presented): The method of claim 19 wherein the encryption key provided by the WPAN is selected from the group consisting of: Kc, which is a 64 bit ciphering key known in the art; Point-to-Point Encryption Send-Key; and Point-to-Point Encryption Recv-Key.